

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~striketrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1-26. (cancelled)

27. (currently amended) A signing apparatus used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions thereof, the apparatus comprising:

a dividing unit which divides the information into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to each all of the data divisions, where the first and second keys are different; and

an appending unit which links the first and second authenticators, and appends the first and second linked authenticators to the information for sending with the information to a certifying apparatus in the authentication system.

28. (currently amended) The signing apparatus according to claim 27, wherein

the dividing unit divides the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

the authenticator creating unit creates the first authenticator by applying the first one-way function using the first key to a first initial value and the first one of the data division divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and the second each of the other data division divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data division divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and the second each of the other data division divisions respectively.

29. (previously presented) The signing apparatus according to claim 27, wherein the appending unit appends authenticators obtained by truncating the first and second authenticators to the information.

30. (previously presented) The signing apparatus according to claim 27, wherein the first and second one-way functions discretely and independently create the first and second authenticators in parallel.

31. (currently amended) The signing apparatus according to claim 27 ~~28~~, wherein intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as an the second initial value to create the second authenticator.

32. (currently amended) A certifying apparatus used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the apparatus comprising:

a separating unit which separates out the information and ~~a plurality of~~ linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

a dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to each all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to each all of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator of the linked authenticators separated out by the separating unit, and by comparing the second authenticator with a fourth authenticator of the linked authenticators separated out by the separating unit.

33. (currently amended) The certifying apparatus according to claim 32, wherein the dividing unit divides the information separated out by the separating unit into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

the authenticator creating unit creates the first authenticator by applying the first one-way

function using the first key to ~~the first~~ a first initial value and one of the data division divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and ~~the second~~ each of the other data division divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and ~~the second~~ each of the other data division divisions respectively.

34. (previously presented) The certifying apparatus according to claim 32, wherein the separating unit obtains truncated authenticators from the data received from the signing apparatus, and the certifying unit compares an authenticator obtained by truncating the first authenticator with the truncated third authenticator separated out by the separating unit, and compares an authenticator obtained by truncating the second authenticator with the truncated fourth authenticator separated out by the separating unit.

35. (previously presented) The certifying apparatus according to claim 32, wherein the first and second one-way functions discretely and independently create the authenticators in parallel.

36. (currently amended) The certifying apparatus according to claim ~~32~~ 33, wherein intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as ~~an~~ the second initial value to create the second authenticator.

37. (currently amended) A signing method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, ~~and creates;~~

creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying

apparatus in the authentication system.

38. (currently amended) A certifying method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

separating out the information and ~~a plurality of~~ linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

dividing the separated out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

authenticating the information by comparing the first authenticator with a third authenticator of the ~~separated out~~ linked authenticators, and by comparing the second authenticator with a fourth authenticator of the ~~separated out~~ linked authenticators.

39. (currently amended) A computer program product for signing in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, ~~and~~;

creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system.

40. (currently amended) A computer program product for certifying in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when

executed by a computer, cause a computer to perform a process, the process comprising:

- separating out the information and ~~a plurality of~~ linked authenticators from authenticator-appended information received from a signing apparatus in the authentication system;

- dividing the separated out information into the plurality of data divisions;

- creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions;

- creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

- authenticating the information by comparing the first authenticator with a third authenticator of the ~~separated-out~~ linked authenticators, and by comparing the second authenticator with a fourth authenticator of the ~~separated-out~~ linked authenticators.

41. (currently amended) An authentication system using authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the system comprising:

- a signing apparatus which includes

- a first dividing unit which divides the information into the plurality of data divisions;

- an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, and which creates a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

- an appending unit which links the first and second authenticators, and appends the ~~first and second~~ linked authenticators to the information for sending with the information to a certifying apparatus in the authentication system; and

- a certifying apparatus which includes

- a separating unit which separates out the information and ~~a plurality of~~ linked authenticators from the authenticator-appended information which is received from the signing apparatus in the authentication system;

- a second dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

- an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator of the linked authenticators separated by the separating unit, and by comparing the second authenticator with a fourth authenticator of the linked authenticators separated by the separating unit.

42. (currently amended) An authentication method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions, ~~and;~~

creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different;

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and ~~a plurality of~~ linked authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to ~~each~~ all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to ~~each~~ all of the data divisions, where the first and second keys are different; and

authenticating the information by comparing the first authenticator with a third authenticator, of the ~~separated-out~~ linked authenticators, and by comparing the second authenticator with a fourth authenticator of the ~~separated-out~~ linked authenticators.

43. (currently amended) A computer program product for authentication in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to each all of the data divisions, ~~and~~;

creating a second authenticator by applying a second one-way function using a second key to each all of the data divisions, where the first and second keys are different;

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and a plurality linked authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to each all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to each all of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator, of the ~~separated-out~~ linked authenticators, and by comparing the second authenticator with a fourth authenticator of the ~~separated-out~~ linked authenticators.

44. (cancelled)

45. (currently amended) An electronic signing method, comprising:

dividing data into a plurality of divisions;

applying a first function to each all of said plurality of divisions using a first key to create a first authenticator and applying a second function to each all of said plurality of divisions using a second key to create a second authenticator; and

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the data.

46. (cancelled)